Data Processing Agreement

Last Updated: March 30, 2026

Effective Date: March 30, 2026

This Data Processing Agreement ("DPA") forms part of the Terms of Use between:

Data Controller (the "Customer")

[Customer Organization Name]

[Customer Address]

[Customer Contact Email]

and

Data Processor (the "Processor")

Sky Made Simple ApS

VAT: DK 43434527

Email: hello@implora.io

Website: https://implora.io

(together as the "Parties")

1. Background & Scope

1.1 Purpose

This DPA governs the processing of personal data by the Processor on behalf of the Customer when using the Implora platform ("Service"). This DPA is mandatory under GDPR Article 28.

1.2 Relationship

Customer is the Data Controller for Microsoft 365 tenant data processed through the Service

Processor acts as Data Processor when processing data on Customer's behalf

This DPA forms part of the Terms of Use

1.3 Precedence

In case of conflict between the Terms of Use and this DPA, the DPA takes precedence on data protection matters.

2. Definitions

"Data Protection Laws" means GDPR (Regulation EU 2016/679), the Danish Data Protection Act (Databeskyttelsesloven), and all applicable EU and Danish data protection legislation.

"Customer Personal Data" means personal data from Microsoft 365 tenants that Processor processes on behalf of Customer, including sign-in logs, user data, device information, and organizational data as described in Annex A.

"Sub-processor" means any third party engaged by Processor to process Customer Personal Data.

"Data Subject" means an identified or identifiable natural person whose personal data is processed.

"Personal Data Breach" has the meaning given in GDPR Article 4(12).

"Supervisory Authority" means the Danish Data Protection Agency (Datatilsynet) or other competent data protection authority.

Terms not defined here have the meanings given in GDPR.

3. Processing Instructions

3.1 Scope of Processing

Processors shall process Customer Personal Data only:

On Customer's documented instructions as set out in this DPA

To provide the Service as described in the Terms of Use

To comply with legal obligations under EU or Danish law

3.2 Processing Details

Details of processing are set out in **Annex A: Processing Details**.

3.3 Customer Instructions

Customer instructs Processor to process Customer Personal Data to:

Execute diagnostic tools on authorized Microsoft 365 tenants

Generate and store security assessment reports

Provide the Service as described in the Terms of Use

3.4 Unlawful Instructions

If Processor believes any instruction violates Data Protection Laws, Processor shall immediately inform Customer. Processor may suspend processing until Customer confirms or amends the instruction.

4. Data Security

4.1 Security Measures

Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, as required by GDPR Article 32, including:

Technical Measures:

Encryption in transit (TLS 1.2+) and rest (Azure Storage encryption)

Multi-tenant data isolation by organization tenant ID

Microsoft Entra ID B2B authentication

Automated security monitoring and alerting

Organizational Measures:

Access restricted to authorized personnel only (least privilege principle)

Confidentiality obligations for all staff with data access

Security awareness training

Incident response procedures

Regular security assessments

4.2 Security Documentation

Processor maintains documentation of security measures and shall make this available to Customer upon reasonable request.

5. Sub-processors

5.1 Authorized Sub-processors

Customer authorizes Processor to engage the Sub-processors listed in Annex B: Sub-processors.

5.2 Sub-processor Obligations

Processor shall:

Impose data protection obligations on Sub-processors equivalent to this DPA

Remain fully liable to Customer for Sub-processor performance

Ensure Sub-processors only process data on Processor's instructions

5.3 Changes to Sub-processors

Processor may add or replace Sub-processors by:

Providing 30 days' prior written notice to Customer (via email or platform notification)

Updating Annex B with current Sub-processor list

Customer may object to a new Sub-processor within 30 days of notification. If Customer objects, Processor shall use reasonable efforts to provide an alternative solution or allow Customer to terminate the affected Service without penalty.

6. Data Subject Rights

6.1 Assistance Obligation

Processor shall assist Customer in responding to Data Subject requests to exercise their rights under GDPR (access, rectification, erasure, restriction, portability, objection).

6.2 Data Subject Requests

If Processor receives a Data Subject request directly, Processor shall:

Promptly notify Customer (within 48 hours)

Not respond to the request except on Customer's documented instructions or as required by law

Provide reasonable assistance to Customer in responding

6.3 Technical Assistance

Processor should provide technical and organizational measures to enable Customer to fulfill Data Subject rights, considering the nature of processing.

7. Personal Data Breaches

7.1 Breach Notification

Processor shall notify Customer without undue delay and in any event within 24 hours of becoming aware of a Personal Data Breach affecting Customer Personal Data.

7.2 Breach Information

Notification shall include:

Nature of the breach (categories and approximate number of Data Subjects and records affected)

Name and contact details of Processor's data protection contact

Likely consequences of the breach

Measures taken or proposed to address the breach and mitigate harm

7.3 Cooperation

Processor shall:

Cooperate with Customer's investigation

Take reasonable steps to mitigate and remediate the breach

Provide timely updates as further information becomes available

Preserve evidence for regulatory or legal proceedings

7.4 Customer Obligations

Customer remains responsible for:

Notifying Datatilsynet within 72 hours (if required under GDPR Article 33)

Notifying affected Data Subjects without undue delay (if required under GDPR Article 34)

8. Data Protection Impact Assessments

Processor shall provide reasonable assistance to Customer with:

Data protection impact assessments (GDPR Article 35)

Prior consultations with Supervisory Authorities (GDPR Article 36)

This applies only to processing of Customer Personal Data and considering the nature of processing and information available to Processor.

9. Deletion & Return of Data

9.1 Deletion upon Termination

Upon termination of the Service, Processor shall:

Delete all Customer Personal Data within 30 days

Delete all backup copies within 90 days

9.2 Exceptions

Processor may retain Customer Personal Data to the extent required by EU or Danish law. Processor shall inform Customer of any such legal retention requirement.

9.3 Certification

Upon Customer's request, Processor shall provide written certification of deletion within 10 business days of completing deletion.

10. Audit Rights

10.1 Information Requests

Processor shall make available to Customer all information necessary to demonstrate compliance with this DPA and GDPR Article 28.

10.2 Audit Procedures

Customer may conduct audits (or engage an independent auditor) to verify Processor's compliance, subject to:

Reasonable prior written notice (at least 30 days)

Conducted during normal business hours

Maximum once per year (unless required by Supervisory Authority or following a Personal Data Breach)

Reasonable measures to minimize disruption

Confidentiality obligations for auditors

10.3 Audit Costs

Customer bears the costs of audits unless the audit reveals material non-compliance.

10.4 Certifications

Processors may provide industry-standard certifications (ISO 27001, SOC 2) as evidence of security compliance in lieu of audit.

11. International Data Transfers

11.1 Data Location

Processor stores Customer Personal Data primarily in Azure Northern Europe (EU region).

11.2 Transfers Outside EU/EEA

If Customer Personal Data is transferred outside the EU/EEA, Processor shall ensure:

- Standard Contractual Clauses (SCCs) approved by the European Commission are in place, or
- The recipient country has an adequacy decision under GDPR Article 45, or
- Other valid transfer mechanism under GDPR Chapter V

11.3 Sub-processor Transfers

Details of Sub-processors located outside the EU/EEA and applicable transfer mechanisms are listed in Annex B.

12. Liability & Indemnification

12.1 Processor Liability

Processor is liable for damages caused by processing that violates GDPR obligations specific to Processors under Article 28.

12.2 GDPR Article 82 Compensation

Each Party shall be liable to Data Subjects for damages under GDPR Article 82 for its respective violations.

12.3 Limitation

Except for GDPR Article 82 compensation to Data Subjects, liability is limited as set out in the Terms of Use.

13. Term & Termination

13.1 Term

This DPA remains in effect for as long as Processor processes Customer Personal Data.

13.2 Survival

Sections 9 (Deletion), 10 (Audit Rights), and 12 (Liability) survive termination.

14. General Provisions

14.1 Confidentiality

Each Party should keep this DPA and related information confidential, except:

Where disclosure is required by law

To enforce this DPA

To professional advisors under confidentiality obligations

14.2 Governing Law

This DPA is governed by Danish law.

14.3 Dispute Resolution

Disputes shall be resolved in the courts of Denmark.

14.4 Amendments

This DPA may only be amended by written agreement signed by both Parties, except that Processor may update Annex B (Sub-processors) in accordance with Section 5.3.

15. Contact Information

Customer Contact:

[Customer Data Protection Contact]

[Customer Email]

Processor Contact:

Sky Made Simple ApS

Email: hello@implora.io

Website: https://implora.io

Supervisory Authority:

Danish Data Protection Agency (Datatilsynet)

Website: https://www.datatilsynet.dk

Email: dt@datatilsynet.dk

Phone: +45 33 19 32 00

Signatures

Customer (Data Controller)

Signature: _

Name: _

Title: _

Date: _

Processor (Sky Made Simple ApS)

Signature: _

Name: _

Title: _

Date: _

Annex A: Processing Details

A.1 Subject Matter

Processing of personal data necessary to provide the Implora platform, including:

Execution of diagnostic tools on Microsoft 365 tenants

Collection and analysis of security assessment data

Generation and storage of security reports

Tenant consent management

A.2 Duration

For the duration of the Service subscription and for 90 days thereafter (to allow for backup deletion).

A.3 Nature and Purpose of Processing

Nature: Collection, storage, analysis, AI-assisted analysis, and presentation of Microsoft 365 tenant data

Purpose: Security assessment, compliance monitoring, risk detection, diagnostic reporting

A.4 Types of Personal Data

Microsoft 365 Tenant Data (Sections 3.6-3.8 of Privacy Policy):

Identity Information:

Email addresses (user principal names)

Full names (display names)

User unique identifiers

User types (member vs. guest users)

Sign-In & Authentication Data:

Sign-in timestamps (30-day history)

IP addresses

Geographic location data (country, city, state, GPS coordinates)

Authentication success/failure status

Applications accessed

MFA methods used per sign-in

Authentication method registrations (may include phone numbers if registered for MFA)

Device Information:

Device names and IDs

Operating system and browser details

Device management status (Entra ID joined, hybrid, registered, unmanaged)

Device compliance and encryption status

Risk & Security Analytics:

Microsoft Identity Protection risk scores

Impossible travel detection

Multi-country access patterns

VPN/proxy usage patterns

Conditional Access policy results

Organizational Data:

Department names

Job titles

Manager relationships

Office locations

Group membership

License assignments

Last password change timestamps

External Collaborator Data:

External user email addresses and names

SharePoint file/folder sharing metadata

Sharing link types and permissions

Access timestamps

And anything related to give insights into the reports generated by the Data Processor on behalf of the Data Controller

Note on AI processing: AI features are opt-in. When the Data Controller uses AI features, tenant data from Microsoft 365 - including security configurations, operational logs, and user identifiers such as email addresses and user principal names - may be transmitted to Anthropic (see Annex B). Anthropic does not train its models on API data and deletes API data within 30 days.

A.5 Categories of Data Subjects

End users within Customer's Microsoft 365 tenants

Customer employees, contractors, and business users

External collaborators and guest users with access to Customer's Microsoft 365 resources

A.6 Processing Operations

Collection (via Microsoft Graph API)

Storage (Azure SQL Database, Azure Blob Storage)

Analysis (automated security assessments)

Reporting (generation of HTML/JSON reports)

Retrieval (customer access to reports)

Deletion (upon termination or customer request)

Annex B: Sub-processors

B.1 Authorized Sub-processors

Sub-processor	Service	Data Location	Transfer Mechanism
Microsoft Azure	Cloud hosting, databases, blob storage, automation	Northern Europe (EU)	EU-based; Microsoft DPA; EU Data Boundary commitment
Dinero	Accounting software (receives organization names only for invoice records)	Denmark (EU)	EU-based; GDPR-compliant DPA
Application Insights (Microsoft)	Performance monitoring, error tracking	Northern Europe (EU)	EU-based; Microsoft DPA
Dynamics 365 (Microsoft)	CRM - customer relationship management (companies, contacts, support cases synced from Intercom via Power Automate)	EU region	EU-based; Microsoft DPA
Intercom	User support and engagement platform	United States	EU-US Data Privacy Framework (DPF) certified; Standard Contractual Clauses (SCCs) as fallback; GDPR-compliant DPA
Anthropic	AI-assisted analysis (opt-in features). When used, tenant data from Microsoft 365 - including security configurations, operational logs, and user identifiers such as email addresses and user principal names - may be transmitted.	United States	Standard Contractual Clauses (SCCs); Anthropic does not train models on API data; 30-day data retention
Mailchimp (Intuit)	Email marketing and service communications	United States	EU-US Data Privacy Framework (DPF) certified; GDPR-compliant DPA

B.2 Sub-processor Obligations

All Sub-processors are contractually bound by:

Data Processing Agreements meeting GDPR Article 28 requirements

Confidentiality obligations

Security measures appropriate to the risk

Assistance with Data Subject rights and breach notifications

B.3 Updates

Processor shall maintain an updated list of Sub-processors at: https://implora.io/legal/sub-processors

Customer will be notified of changes via email or platform notification 30 days in advance, as per Section 5.3 of this DPA.

End of Data Processing Agreement